DEMO: Radio Unit Activity Fingerprinting through Electromagnetic Side-Channel Analysis in O-RAN Networks

Sreenithya Somavarapu
George Mason University
Fairfax, VA, USA
ssomavar@gmu.edu

Harshita Chaudhari
George Mason University
Fairfax, VA, USA
hchaudh7@gmu.edu

Nour El Houda Aidlaid
George Mason University
Fairfax, VA, USA
naidlaid@gmu.edu

Nongnapat Adchariyavivit
George Mason University
Fairfax, VA, USA
nadchari@gmu.edu

Qais Dib
George Mason University
Fairfax, VA, USA
qdib@gmu.edu

Moinul Hossain
George Mason University
Fairfax, VA, USA
mhossa5@gmu.edu

Vijay K. Shah
North Carolina State University
Raleigh, NC, USA
vijay.shah@ncsu.edu

Md. Tanvir Arafin
George Mason University
Fairfax, VA, USA
marafin@gmu.edu

ABSTRACT

While the disaggregated architecture of the industry-driven Open Radio Access Network (O-RAN) promises to foster vendor competition, accelerate innovation, and reduce cost for 5G/6G cellular network deployments, it also exposes the cellular network to various new cybersecurity and privacy vulnerabilities. This demo paper highlights one such new potential cybersecurity vulnerability in the Radio Unit (RU) of O-RAN networks, where an adversary can infer RU activity by analyzing electromagnetic side-channel emissions. We present a custom-built, open-source cellular O-RAN testbed equipped with EM measurement capabilities that enables direct observation of the FPGA-based RU during operation. By capturing EM emissions from the RU, we extract side-channel traces that reveal the underlying RU activity. These traces are then analyzed using a Random Forest-based machine learning classifier, which accurately distinguishes between different RU activity patterns. Our preliminary findings demonstrate the feasibility of inferring RU-level operations via passive EM observation, highlighting a previously unexplored security threat in O-RAN systems. All code and experimental artifacts are made publicly available at https://github.com/SPIRE-GMU/NextGRadio_Sidechanel.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

Fifth Generation (5G) Network, Machine Learning (ML), Open Radio Access Network (O-RAN), Side-Channel Analysis

WiSec 2025, June 30-July 3, 2025, Arlington, VA, USA

ACM ISBN 979-8-4007-1530-3/2025/06
https://doi.org/10.1145/3734477.3736152

ACM Reference Format:
Sreenithya Somavarapu, Harshita Chaudhari, Nour El Houda Aidlaid, Nongnapat Adchariyavivit, Qais Dib, Moinul Hossain, Vijay K. Shah, and Md. Tanvir Arafin. 2025. DEMO: Radio Unit Activity Fingerprinting through Electromagnetic Side-Channel Analysis in O-RAN Networks. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025), June 30-July 3, 2025, Arlington, VA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3734477.3736152

1 INTRODUCTION AND MOTIVATION

Contemporary 5G systems are undergoing a major architectural shift with the adoption of Open Radio Access Network (O-RAN). Unlike traditional cellular networks, O-RAN enables an open, disaggregated, and virtualized radio access network (RAN) design. This enables operators to integrate hardware and software from multiple vendors, enhancing flexibility, scalability, cost efficiency, and competition, ultimately benefiting consumers.

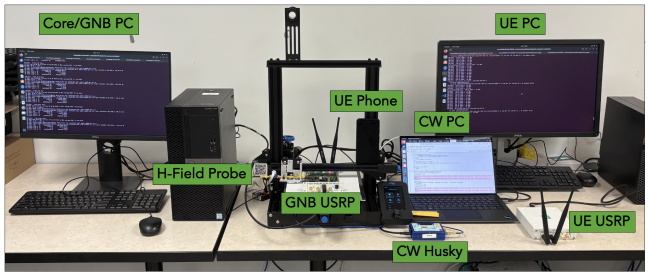

Figure 1: EM side-channel setup on a 5G O-RAN testbed with a core network, RU (gNB USRP), nrUE (USRP B210), and COTS UE (Pixel 5). EM signals are captured using an H-field probe and the ChipWhisperer Husky.

However, the disaggregation of 5G components—through separate radio units (RUs), distributed units (DUs), and central units (CUs)—has led to high-density RU deployments in unsecured, open environments. This creates a new attack vector where adversaries

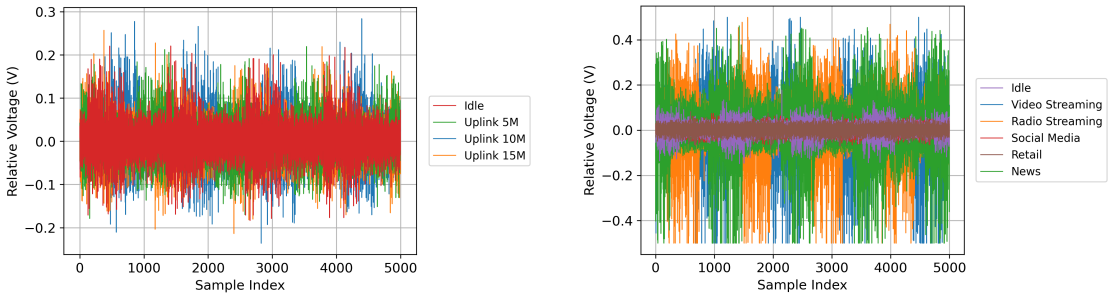

Figure 2: Relative EM emission traces collected from the base station FPGA during different user activities. The left subfigure shows the collected traces when the nrUE was involved in uplink data transmission at different bandwidths. The right subfigure plots traces collected for the gNB USRP when the COTS UE (Pixel 5) was involved in different application activities.

can mount side-channel attacks by passively capturing electromagnetic (EM) emissions from RU FPGAs using EM probes[2]. Combined with machine learning, these emissions have been used to fingerprint FPGA activity, expose sensitive data, and compromise systems. Yet, RU devices (e.g., software-defined radios) remain largely unevaluated for such vulnerabilities. To address this, our demo introduces an EM fingerprinting approach to identify RU activity triggered by mobile devices. This method can assess and benchmark the side-channel exposure of various commercial RUs based on privacy risk.

2 5G O-RAN TESTBED DESIGN AND SETUP

Our 5G O-RAN testbed is built using the open-source OpenAirInterface (OAI) stack [1]. A USRP B210 radio is used for its broad frequency support, and both the 5G core and gNodeB (gNB) run on an Ubuntu 22.04 desktop. The gNB is deployed following the O-RAN split as separate CU and DU components. The testbed includes two types of user equipment (UEs): a software-defined UE and a commercial off-the-shelf (COTS) smartphone. Figure 1 shows the complete setup.

This work aims to analyze electromagnetic (EM) signatures from the radio unit (RU) to identify network behavior. EM signals are captured from the RU's FPGA chip, housed in the gNB USRP. To ensure minimal noise, the H-field probe is positioned 2–3 inches above the exposed FPGA using a modified 3D printer mount. Importantly, *we measure computation-induced EM leakage from the FPGA—not RF emissions—at the RU level.*

3 RESULTS AND DISCUSSIONS

Distinct EM patterns were observed at the RU corresponding to different UE activities. An idle baseline was used to identify meaningful variation. Traffic was generated using *iPerf* at fixed 1500-byte packets and varying bandwidths. Figure 2 (left) shows traces from the nrUE during uplink transmission. Figure 2 (right) shows traces from the COTS UE (Pixel 5) emulating typical app usage. For each configuration, 1,400 EM traces were collected for training and testing.

Two machine learning models were used for classification. First, binary classifiers were trained on each pair of activity states (e.g., idle vs. video streaming), improving performance when class overlap was limited. Then, a random forest multiclass model classified all activity types simultaneously, enabling broader scalability. Classification results are shown in Table 1. Full implementation details are available in our repository [3].

Activity	Precision	Recall	F1-Score	Support
Idle	1.00	0.75	0.86	4
News sites	1.00	1.00	1.00	3
Radio station streaming	1.00	1.00	1.00	3
Retail sites	1.00	1.00	1.00	9
Social media sites	1.00	1.00	1.00	4
Video streaming	0.50	1.00	1.00	1
Uplink 5M	1.00	1.00	1.00	4
Uplink 10M	0.80	0.80	0.80	5
Uplink 15M	0.80	0.80	0.80	5

Table 1: Accuracy of a random-forest based multiclass classifier in differentiating user behavior from side-channel traces collected at the base-station.

4 CONCLUSIONS

In this work, we explored whether electromagnetic (EM) emissions from the hardware components, conducted in low-noise lab conditions, of a 5G O-RAN radio unit (RU) leak information related to user equipment (UE) activity. Our initial experiments confirm the presence of a reliable EM side channel that can be exploited to fingerprint RU-level operations and infer user activity patterns. These findings underscore a previously overlooked cybersecurity risk in O-RAN architectures and motivate further investigation into side-channel defenses for next-generation wireless systems.

5 ACKNOWLEDGMENTS

The Commonwealth Cyber Initiative grant #N-3Q24-002 supported this project. The authors thank Prof. Jair Ferrari, Azuka Chiejina, and Abiodun Ganiyu for their help and support.

REFERENCES

[1] OpenAirInterface. [n. d.] 5G Core Network - OpenAirInterface. https://openairinterface.org/oai-5g-core-network-project/. Accessed: 2025-04-28. ().

[2] Sameer Kumar Singh, Rohit Singh, and Brijesh Kumbhani. 2020. The evolution of radio access network towards open-ran: challenges and opportunities. In *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 1–6. DOI: 10.1109/WCNCW48565.2020.9124820.

[3] SPIRE-GMU. [n. d.] NextG Radio Side Channel. https://github.com/SPIRE-GMU/NextGRadio_Sidechanel. Accessed: 2025-04-28. ().